QUICK USER GUIDE

Audit & Risk Management Platform

A practical, beginning-to-end walkthrough for new users — what to do after you sign in, and what comes next at every stage of the audit lifecycle.

Version 1.3 · October 2026
Audit & Risk Management Platform

Contents

1. Getting Started
2. Initial Tenant Setup
3. End-to-End Audit Lifecycle
4. Dependencies — What the System Enforces
5. Risk → Plan → Engagement, Explained
6. Findings — Frequently Asked Questions
7. Engagement → Finding → Follow-Up
8. What Do I Do Next? (Cheat Sheet)
9. Recommended User Journey
10. Quick Reference
11. Audit Intelligence — AI-Assisted Drafting and Review

1. Getting Started

The platform is multi-tenant: each customer organization is an independent tenant. Access is layered:

Platform Administrator

A cross-tenant authority, held as a platform-level (realm) role in the identity provider — not tied to any one organization. Can create brand-new organizations (tenants) and each one's first System Administrator. Cannot otherwise act inside an organization's day-to-day audit work.

Location · Admin → Organizations (`/admin/organizations`)

Tenant / System Administrator

Full control within their own organization only: creates further users of any role (including additional System Administrators), configures reference data, departments, risk matrix, etc.

Location · Admin → Users (`/admin/users`)

Ordinary / Auditor Users

Created by a System Administrator and assigned one or more functional roles (see table below). Their menu and permissions adjust automatically to what their role(s) allow.

Creating Additional Tenant Administrators

An existing System Administrator adds a new user via Admin → Users and assigns them the System Administrator role. Creating a brand-new organization (a second tenant) instead requires a Platform Administrator.

Built-in Roles (seeded automatically for every new tenant)

Role	Typical footprint
System Administrator	Full ownership of the tenant — every module, including user management and permissions.
Chief Internal Auditor	Owns the audit lifecycle end to end (universe through reporting); can approve/close; view-only on administration.
Audit Manager	Runs the audit program day to day; same footprint as CIA minus deletion rights and administration visibility.
Auditor	Fieldwork: create/edit execution, working papers and findings; view elsewhere for context.
Risk Manager	Owns the Risk Register end to end; view-only elsewhere.
Department Head	Reviews and responds to findings/follow-up affecting their department; view-only otherwise.
Management Action Owner	Owns their assigned management action plans and follow-up items.
Audit Committee Viewer / Executive Viewer	Read-only oversight across the lifecycle, with export where available.

Login & Basic Setup

1. Open the Audit & Risk Platform at `https://audit.thinkfinancials.com` and sign in — authentication is handled by your organization's identity provider.
2. Sign in using the credentials provided by your administrator. Your menu and permissions are determined by the role(s) your administrator has assigned to your account (see the role table above).
3. After signing in, open **Audit Journey** in the Dashboard menu (`/journey`). This is a live, auto-generated checklist — it reads your organization's real data and tells you exactly which lifecycle stage is next. Use it throughout as your compass.

2. Initial Tenant Setup

When a Platform Administrator creates a new organization, a standard baseline is provisioned automatically in one transaction — a new tenant is never left half-configured.

Already pre-populated for a new tenant

Item	Details
Roles	All 9 built-in roles above, with their default permission grants.
Risk Matrix	A default 5×5 Likelihood × Impact matrix with Low/Medium/High/Critical bands. Editable afterwards.
Audit Universe Categories	Department, Function, Process, Project, Branch, Program, IT System, Vendor.
Reference Data	~17 lookup categories pre-filled — Risk Type/Rating/Appetite, Location, Audit Type/Frequency/Status, Engagement Status, Finding Category/Status/Priority, Root Cause Category, Recommendation Category, Action Status, Follow-Up Status, Document Type, Evidence Type, Engagement Team Role.
Departments & Business Units	A generic enterprise baseline — 20 Departments and ~60 Business Units/Processes — so dropdowns are never empty on day one.
Risk Categories	Strategic, Operational, Financial, Compliance, IT, Cybersecurity, Fraud, Reputational — shared across all organizations, not tenant-specific.

What the Administrator still configures

Item	Why it starts empty
Audit Universe entities (the actual auditable subjects)	Every organization's business processes/systems are unique — nothing is auto-created here.
Organization Structure (Group → Entity → Business Unit → Department → Location)	A newer, optional hierarchy layered above the legacy Departments/Business Units, which already work out of the box.
Additional Users & role assignments	Only the first System Administrator exists initially.
Risk Register, Audit Plans, Engagements, Findings	All lifecycle data — intentionally empty until your team starts working.
Customization of the seeded matrix / reference data / departments	The defaults are a usable starting point, not a fixed requirement — all editable under Administration.

> **BULK IMPORT**
>
> Admin → Bulk Import (`/admin/import`) accepts spreadsheets for Departments, Auditable Entities, the Risk Register, Audit Plans, Planned Audits, Engagements, Findings, and Management Action Plans — useful for loading an existing register instead of entering everything by hand.

3. End-to-End Audit Lifecycle

The application itself tracks progress through 14 stages (see the Audit Journey page) — the sequence below is the recommended path through them.

1 Audit Universe → **2** Risk Assessment → **3** Annual Plan → **4–5** Planned Audit + Team →
6 Engagement → **7** Audit Program → **8** Working Papers → **9–11** Findings + Response + Action Plan →
12 Follow-Up → **13–14** Closure + Reporting

Stage-by-stage

> **1 — Audit Universe · `/universe`**
> **What:** The catalog of auditable subjects (departments, processes, systems, vendors…). **Why:** Everything downstream — risks, planned audits — points back to an entity here. **Before starting:** Nothing (categories are pre-populated). **Next:** Assess risk against these entities, or plan an audit directly.

> **2 — Risk Assessment · `/risks`, `/risks/heatmap`**
> **What:** Score risks (Likelihood × Impact) using the tenant's Risk Matrix. **Why:** Gives the Annual Plan an objective basis for prioritization. **Before starting:** Nothing technical is required — Risk Category and Risk Matrix already exist. **Next:** Optionally link the risk to an Audit Universe entity, then use the resulting rating to inform planning (see Section 5).

> **3–5 — Annual Audit Plan, Planned Audits, Team Assignment · `/planning`**
> **What:** A yearly Plan (Draft → Approved → Active) containing individual Planned Audits, each tied to one Audit Universe entity, quarter and budget, with a tentative lead auditor/team. **Why:** Turns risk insight into a scheduled, resourced program of work. **Before starting:** An Audit Universe entity for each Planned Audit. **Next:** Approve the Plan, assign a team, then convert the Planned Audit into an Engagement.

> **6 — Engagement · `/engagements`**
> **What:** The executable unit of audit work — status flows Planning → Fieldwork → Review → Reporting → Closed. **Why:** Everything auditors actually do (working papers, findings) happens under an Engagement. **Before starting:** Nothing technically — see Section 5 for how it relates to Plans. **Next:** Optionally attach an Audit Program, then start fieldwork.

> **7 — Audit Program · `/programs`**
> **What:** A reusable library of procedure templates (steps, risks addressed, controls tested, testing method) that can be cloned onto an Engagement. **Why:** Standardizes fieldwork. **Before starting:** Nothing. **Next:** Attach a template when creating/editing the Engagement, or proceed without one. If your organization has Audit Intelligence, you can also generate a draft program for an engagement, or review its existing program (Section 11.3 F and G).

> **8 — Working Papers & Evidence · inside an Engagement**
> **What:** Documented procedures, conclusions, evidence files and reviewer comments, scoped to one Engagement. **Why:** The audit trail behind every finding. **Before starting:** An Engagement must exist. **Next:** Raise Findings from what you observe.

> **9–11 — Findings, Management Response, Action Plan · `/findings`, `/followup`**
> **What:** Record an exception, capture management's formal response, then a Management Action Plan (owner, due date, status). **Why:** This is the corrective-action record the whole audit exists to produce. **Before starting:** An Engagement. **Next:** Track the action plan to completion, then verify it.

> **12 — Follow-Up · `/followup`**
> **What:** A Follow-Up Review records whether management's action was actually implemented. **Why:** Closes the loop — findings are not closed on management's word alone. **Before starting:** A Finding (ideally with a completed Action Plan). **Next:** Close the Finding, or re-open it if verification fails.

> **13–14 — Closure & Reporting · `/reporting`**
> **What:** Close the Finding/Engagement once verification requirements are satisfied, then communicate results. **Why:** Formal sign-off and stakeholder communication. **Before starting:** Verified/closed findings for the fullest report. **Next:** Review Dashboards, build/export a report.

4. Dependencies — What the System Actually Enforces

System-enforced dependency = the application will not let you proceed without it (a database foreign key or explicit validation). **Recommended audit practice** = normally you should do this first, but the application does not block you if you skip it.

Module	Required before starting	Status	Next step
Audit Universe entity	An Audit Universe Category (pre-populated)	INDEPENDENT starting point	Assess risk / plan an audit against it
Risk (Risk Register)	Risk Category & Risk Matrix (both pre-populated). Linking to an entity is optional.	SYSTEM for Category/Matrix (already satisfied) · OPTIONAL entity link	Use the rating to help prioritize the Annual Plan
Annual Audit Plan (header)	Nothing	INDEPENDENT	Add Planned Audits
Planned Audit (line item)	An Audit Universe entity	REQUIRED BY SYSTEM	Assign a lead auditor / team
Team Assignment	A Planned Audit	RECOMMENDED (drives the Journey checklist; not enforced)	Convert to an Engagement
Engagement	Nothing — Plan / Planned Audit / Entity link is optional	RECOMMENDED to originate from a Planned Audit · can be standalone	Attach a program, begin fieldwork
Audit Program (attached template)	Nothing	OPTIONAL	Build Working Papers
Working Paper / Evidence	An Engagement	REQUIRED BY SYSTEM (Engagement) · OPTIONAL program-step link	Raise a Finding
Finding	An Engagement	REQUIRED BY SYSTEM (Engagement) · OPTIONAL Working Paper link · no Risk link exists at all	Management Response
Management Response	An existing Finding	REQUIRED BY SYSTEM	Management Action Plan
Management Action Plan	An existing Finding	REQUIRED BY SYSTEM	Follow-Up Review
Follow-Up Review	An existing Finding (Action Plan link optional)	REQUIRED BY SYSTEM (Finding) · OPTIONAL Action Plan link	Verify / close
Dashboards	Nothing	INDEPENDENT read-only view	—
Reporting Center	Nothing (reports reflect whatever data exists)	INDEPENDENT	—

5. Risk → Plan → Engagement, Explained

This is the part new users find confusing most often, so here it is plainly:

> Creating a Risk does **not** automatically create, update, or feed into any Audit Plan. There is no automatic linkage in either direction.

1. A Risk may optionally be linked to one Audit Universe entity. When it is, that entity's own risk rating is automatically recalculated from its linked risks.
2. That rating is advisory only. Auditors use it as a manual reference when deciding which entities deserve a Planned Audit — the system never auto-selects or forces anything into the Plan based on risk scores.
3. Building the Annual Plan means manually adding Planned Audits against Audit Universe entities — not against Risks directly. There is no "convert this Risk into a Planned Audit" action.
4. A Planned Audit becomes an Engagement only through an explicit "Create Engagement" action (from the Planning screen). Doing so copies over the entity, dates, budget and team. The system blocks creating a second Engagement from the same Planned Audit, but does not require going through one at all.
5. An Engagement can be created directly and independently — with no Plan, no Planned Audit and no Audit Universe entity — for ad-hoc or investigative work.

Recommended approach

Audit Universe → score entities under Risk Assessment → build the Annual Plan by adding Planned Audits for the higher-risk entities → assign a team → approve → convert to an Engagement. Reserve standalone Engagements for investigations or special requests that fall outside formal, risk-based planning.

6. Findings — Frequently Asked Questions

Question	Answer
Can I create a Finding without first creating a Risk?	Yes. Findings have no relationship to Risks in the data model at all — there is no way to link one to the other. Not currently supported.
Can I create a Finding without an Audit Engagement?	No. Every Finding must belong to an Engagement — system-enforced.
Can I create a Finding directly from Findings Management?	Yes — pick an existing Engagement. You do not have to create a Working Paper first (that link is optional).
Can Findings be imported?	Yes, via Admin → Bulk Import, alongside Risks, Audit Plans, Planned Audits, Engagements, Departments, Auditable Entities and Action Plans.
What relationships are mandatory?	Only Finding → Engagement. Working Paper, Responsible Department / Org Unit / Business Unit, and Finding Theme are all optional.
Recommended route for findings from an audit?	Engagement → Working Paper (procedures/evidence) → Finding raised from it → Management Response → Action Plan → Follow-Up.
Can findings be followed up independently?	A Follow-Up Review always needs a Finding, but the Management Action Plan it verifies is optional — so yes, a review can be recorded straight against a Finding. The recommended path is still Finding → Response → Action Plan → Follow-Up against that plan.

7. Engagement → Finding → Follow-Up

The practical, end-to-end fieldwork lifecycle — every step below exists in the current application:

Engagement → (optional) Audit Program → Working Papers / Evidence → Finding → Recommendation → Management Response → Management Action Plan → Follow-Up Review → Closure

> NOTE
> The app does not have a separate "Procedures / Testing" record distinct from a Working Paper — testing detail (objective, procedure, testing method, sampling method) is captured directly on the Working Paper and on the Audit Program Step it may reference.

8. What Do I Do Next? — Cheat Sheet

> **If you have just created a Risk**
> Optionally link it to an Audit Universe entity → use the resulting rating as input when you build or update the Annual Audit Plan.

> **If you have created an Audit Plan**
> Add Planned Audits (pick entities, quarter, budget) → assign a lead auditor/team → Approve the plan.

> **If you have created an Engagement**
> Optionally attach an Audit Program template → start adding Working Papers as fieldwork proceeds.

> **If you have created a Finding**
> Record Root Cause and Recommendation → capture Management's Response → add a Management Action Plan with an owner and due date.

> **If you want to test Follow-Up**
> Open a Finding whose Action Plan is "Completed" → go to Follow-Up → add a Follow-Up Review with an Implementation Status → if "Implemented", close the Finding.

9. Recommended User Journey

Follow this single scenario from beginning to end to exercise every major module — no random clicking required.

1. Sign in and open Audit Journey (`/journey`) — your live checklist for the rest of this walkthrough.
2. Review pre-populated master data: Departments, Business Units, Reference Data (Admin).
3. Review the Audit Universe (`/universe`) — add one Auditable Entity if none exist.
4. Create a Risk (`/risks`) and link it to that entity.
5. Open Annual Audit Planning (`/planning`), create a Plan, and add a Planned Audit for that entity.
6. Assign a lead auditor / team to the Planned Audit, then Approve the Plan.
7. Convert the Planned Audit into an Engagement (`/engagements`).
8. Optionally attach an Audit Program template (`/programs`).
9. Add a Working Paper with a piece of evidence, inside the Engagement.
10. Create a Finding (`/findings`) from the Engagement.
11. Record a Management Response, then add a Management Action Plan.
12. Perform a Follow-Up Review (`/followup`) and close the Finding.
13. Review the Dashboards (`/dashboards` — Executive, Chief Internal Auditor, My Dashboard, Risk, Resources).
14. Generate a report from the Reporting Center (`/reporting`).

10. Quick Reference

I want to…	Go to…	Do I need anything first?
Create a Risk	Risk Register — `/risks`	No. Risk Category & Matrix are pre-populated; linking to an entity is optional.
Plan an Audit	Annual Audit Planning — `/planning`	No, to create the Plan itself. Each Planned Audit inside it needs an Audit Universe entity.
Create an Engagement	Engagements — `/engagements`	No. Can be standalone, or converted from an approved Planned Audit (recommended).
Build an Audit Program	Audit Programs — `/programs`	No. Build anytime; attach to an Engagement whenever you like (optional).
Record a Finding	Findings — `/findings`	Yes — an existing Engagement.
Follow up a Finding	Follow-Up — `/followup`	Yes — an existing Finding (ideally with a Management Action Plan).
View results	Dashboards — `/dashboards`	No.
Generate reports	Reporting Center — `/reporting`	No.
Draft or review with Audit Intelligence	See Section 11	Yes — your organization's package must include it, it must be switched on, and you need the permission for the underlying action.

Generated from the current application source (backend domain model, services and navigation) as of October 2026. If a screen's behavior appears to differ from this guide, treat the running application as authoritative and flag the discrepancy to the Product Owner.

11. Audit Intelligence — AI-Assisted Drafting and Review

11.1 What Audit Intelligence is

Audit Intelligence is the platform's built-in drafting assistant. From facts you supply (and, in some workflows, records already in the platform) it prepares a **draft** (or, for an existing audit program, a set of **suggestions**) for you to review. It supports — and never replaces — the auditor's professional judgement.

- **It is not ordinary application functionality.** Normal screens store and calculate exactly what you enter. Audit Intelligence generates new wording and suggestions that may be incomplete, inaccurate or unsuitable for your engagement.
- **Nothing is saved or issued automatically.** Every workflow below shows a draft, lets you edit or discard it, and takes effect only when you explicitly apply or save it using the platform's normal controls.
- **Human approval is mandatory.** You remain responsible for every fact, rating, cause, recommendation and conclusion.

11.2 Access and availability

Audit Intelligence controls appear only when **all** of the following are true:

1. **Your organization's subscription package includes it.** In Admin → Organizations each organization shows "Audit Intelligence: included / not included". The Starter package does not include it; the Professional and Enterprise packages do. When it is excluded, the screens show the notice "Audit Intelligence is not included in your subscription" instead of the buttons.
2. **It is switched on for the environment** and a provider is configured. This is a deployment setting managed by your platform operator, not a per-user option. If it is off, the buttons are not shown.
3. **You hold the permission for the action the draft feeds** (see the table below). The platform checks the same permission it needs to save the result.

Workflow	Where the control appears	Permission needed (module · action)
Risk drafting	Risk Register → + Add Risk	Risk Register · Create
Finding generation	Engagement detail page → Generate finding from template	Findings · Create, plus Audit Execution · View (working-paper context also needs Working Papers · View)
Objectives & scope	New Engagement and Edit Engagement forms	Audit Execution · Create (new) or Edit (existing engagement that is not Closed)
Audit program generation	Engagement detail page → Generate Audit Program with Audit Intelligence	Audit Execution · Edit, Audit Programs · Create and Risk Register · View (the engagement must not be Closed)
Audit program review	Engagement detail page → Review Audit Program with Audit Intelligence (only when the engagement has a linked audit program)	Audit Execution · Edit and Audit Programs · Edit. Risk Register · View is *not* required; without it the review runs without risk context.
Report & presentation narrative	Engagement → Audit report & executive presentation → Narrative	Reporting · Export, plus Findings · View and Audit Execution · View

Roles differ. For example, a user with the default Auditor role sees the finding button on an engagement but does not see Add Risk, and sees no narrative or export buttons on the report page, because that role does not hold Risk Register · Create or Reporting · Export in the tested tenant. Your System Administrator can adjust role permissions.

> IF A CONTROL IS MISSING
>
> Check, in this order: (1) is the notice about your subscription showing? Ask your administrator about the package; (2) do your roles include the permission above? Ask your System Administrator; (3) otherwise Audit Intelligence may be switched off or temporarily unavailable — try later, then contact your administrator.

Restricted engagements. Content of a restricted (special assignment) engagement is sent to an external provider only if a System Administrator has allowed this under Admin → Restricted assignments. It is off by default; without it, requests for that engagement are refused.

Usage limits. Requests are limited per user per minute and per day. If you reach a limit the screen says to wait a minute or to try again tomorrow.

11.3 Step-by-step workflows

> A. Risk drafting
> **Purpose:** draft a risk statement, causes, consequences, suggested scoring and rationale from a short risk title.
> **Path:** Risk Register (`/risks`) → **+ Add Risk**.
> **Input:** type a short title in the **Risk** box.
> **Action:** click ✦ **Generate with Audit Intelligence**.
>
> **Review:** an "✦ Audit Intelligence draft" panel appears with Risk Statement, Causes, Consequences, AI-suggested Controls, Suggested Scoring (likelihood, impact, control effectiveness), Scoring Rationale and, where available, a Suggested Category. Projected inherent/residual scores are calculated by the platform's scoring model from the suggested ratings, not by AI. **Nothing is ticked by default** — tick each part you want. Suggested controls are not verified: they are copied into Existing Controls only if you also tick "I have verified these controls exist".
>
> **Continue:** click **Use Draft** to fill the form (or **Discard**), edit any field, then click **Save Risk**. The draft is not saved until you do.
>
> **Limits:** the screen states that only the text you enter on it is sent. Input length is capped. Do not include content from a restricted assignment — the Risk Register is not restricted.

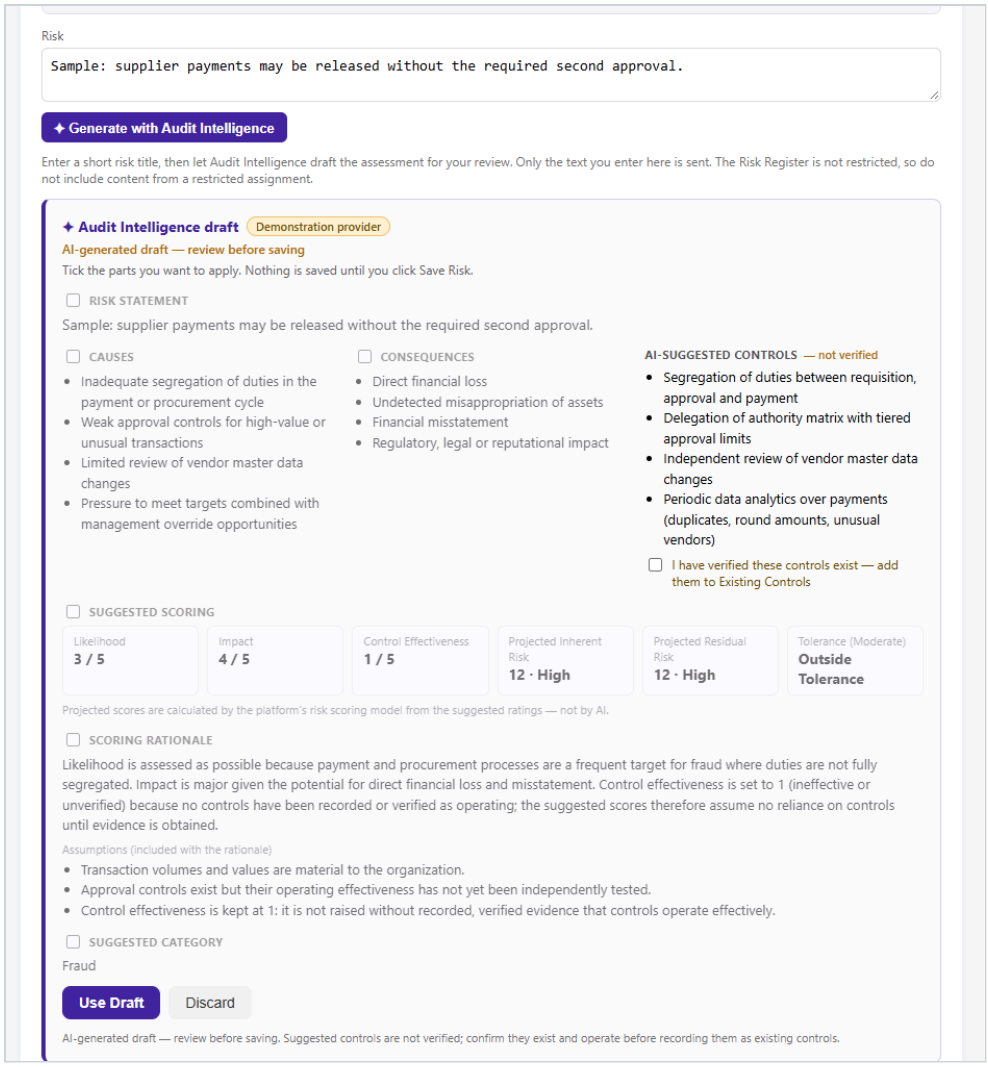


Figure 1 — Risk drafting. The draft panel starts with every section unticked. The "Demonstration provider" badge appears only when the environment uses the built-in sample provider; its output is illustrative.

B. Audit finding generation

Purpose: turn your observation into a structured draft finding (condition, criteria, cause, effect, recommendation, rating and optionally a management response).
Path: Engagements → open an engagement → **Generate finding from template** → **✦ Generate finding with Audit Intelligence**.
Input: choose a **Finding template**; describe **What did you observe? (facts only)** (at least 10 characters, up to 4,000); optionally Criteria, Audit procedure performed, Working paper and its evidence, "Draft a management response from notes I provide", Action owner and Target date.
Action: click **Generate draft** (use **Cancel** to stop a request).

Review: your source information is shown beside the editable draft. Check **Missing information**, **Not verified — confirm or remove** and **Follow-up questions**. Where criteria were not supplied they are flagged, not invented; a cause may be labelled a hypothesis or "not established". Edit any field and choose the Risk rating (a rating is suggested with a rationale).

Continue: tick **I have verified the facts and evidence in this draft**, then click **Save as draft finding** (or **Discard draft**). The finding is saved with status **Draft** and is not issued to management until you change its status; you then continue with the usual Management Response, Action Plan and Follow-Up.

Limits: evidence **file names** are shared with Audit Intelligence; file contents are not. Include figures, dates and names only if verified.

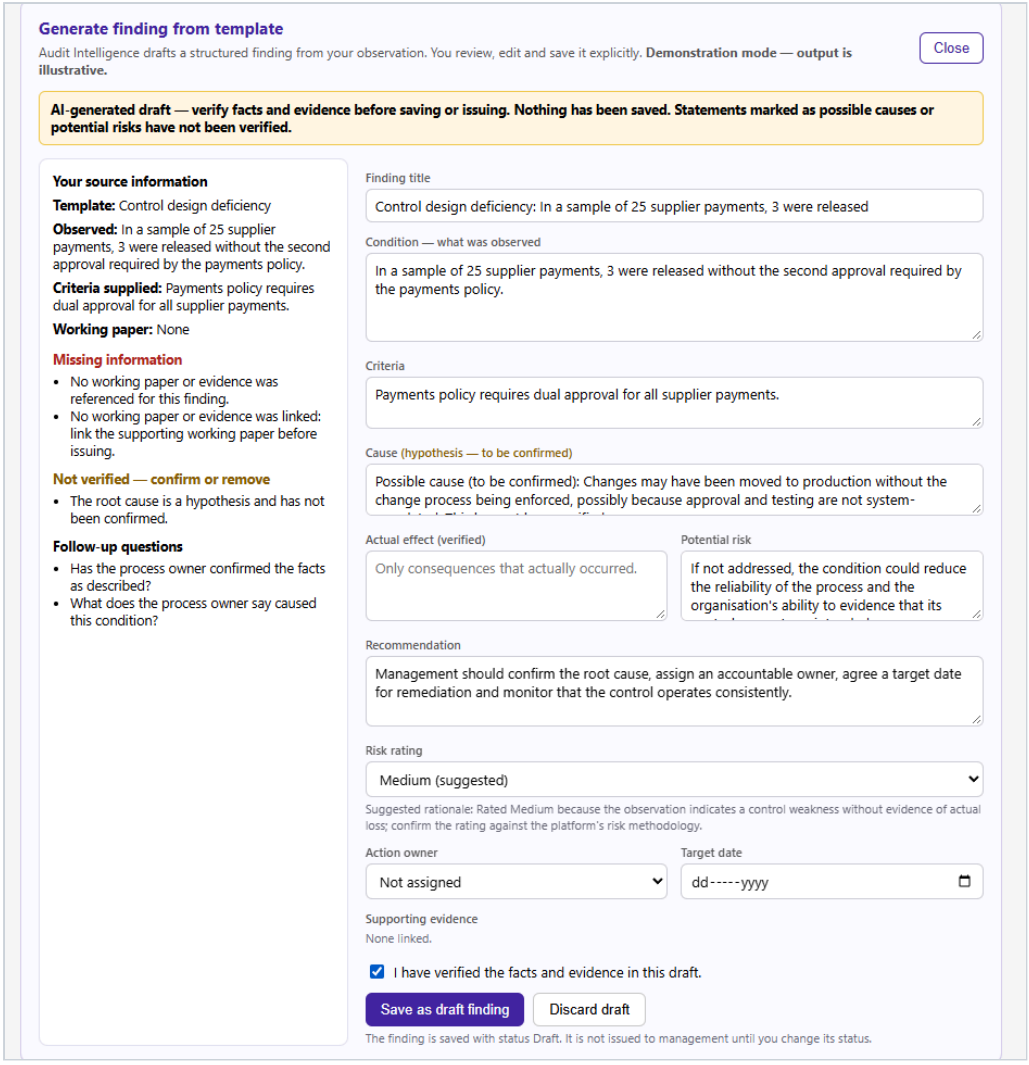


Figure 2 — Finding draft review. Your source information and the flagged gaps sit beside the editable draft; saving requires the verification tick.

C. Audit objectives and scope refinement

Purpose: draft, or improve, an engagement's Objective and Scope.
Path: Engagements → New Engagement, or open an engagement → edit it.
Input: engagement name, type, financial year and Audit Universe item; if Objective/Scope already contain text, that text is used and its points kept.
Action: ✦ **Draft with Audit Intelligence** when the fields are empty, or ✦ **Refine with Audit Intelligence** when text exists.

Review: a side-by-side **Current** and **Proposed (editable)** view for Objective and Scope, with "What was retained", "Material changes" and "Assumptions and information gaps". Tick the field(s) to apply.

Continue: click **Apply to form** (or **Dismiss**). Applying only fills the form; click **Create Engagement** (new engagement) or **Save Changes** (existing engagement) to keep it. If you edited the fields after generating, the button reads **Replace with proposal**.

Limits: the proposal is based on the engagement details and, if you can view the Risk Register, risks linked to the Audit Universe item. Without a linked item there is little context — the assumptions list says so.

In an existing engagement, open it and choose the edit option: because Objective and Scope already contain text, the same button reads ✦ **Refine with Audit Intelligence**.

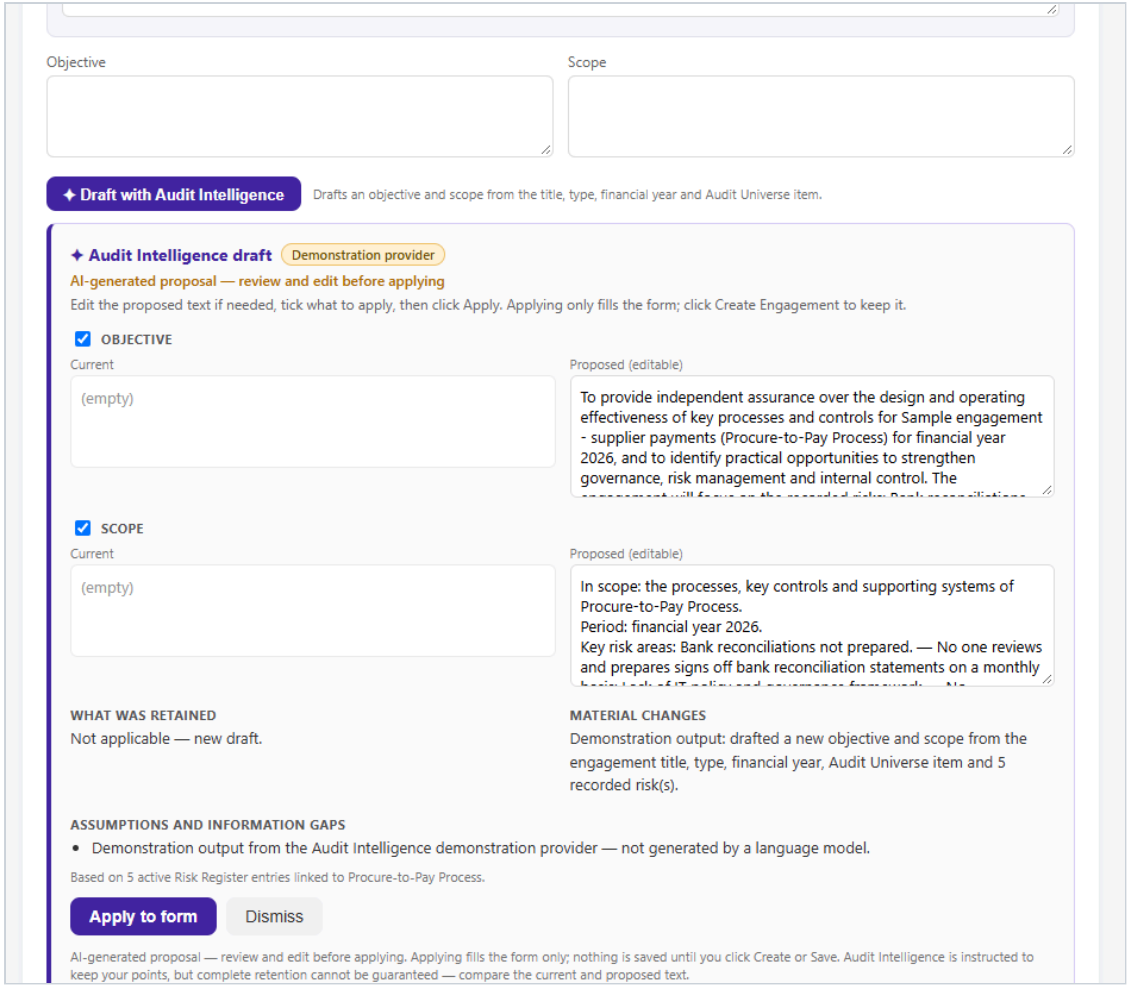


Figure 3 — Objectives and scope proposal on the New Engagement form (current versus proposed, editable). Nothing is saved until Create Engagement.

D. Audit report narrative drafting

Purpose: draft the narrative parts of an audit report: executive summary and key messages, limitations, next steps and — only where the evidence supports it — a *proposed* conclusion.
Path: open an engagement → **Audit report & executive presentation** →; choose **Formal audit report**, then the findings and sections to include ("1. What to produce").
Action: in "2. Narrative (your words)" click **Draft narrative with Audit Intelligence**.

Review: a draft is shown with its warning and any caveats. If the evidence does not support a conclusion, it says so and you must provide your own. Click **Use this draft** to copy it into the editable fields (or **Discard**), then edit the Executive summary, Overall conclusion, Limitations and Next steps.

Continue: the conclusion is never pre-confirmed. Tick **I confirm this is the audit conclusion, supported by the evidence** only when it is. Use **Preview**, then the export controls (see 11.5).

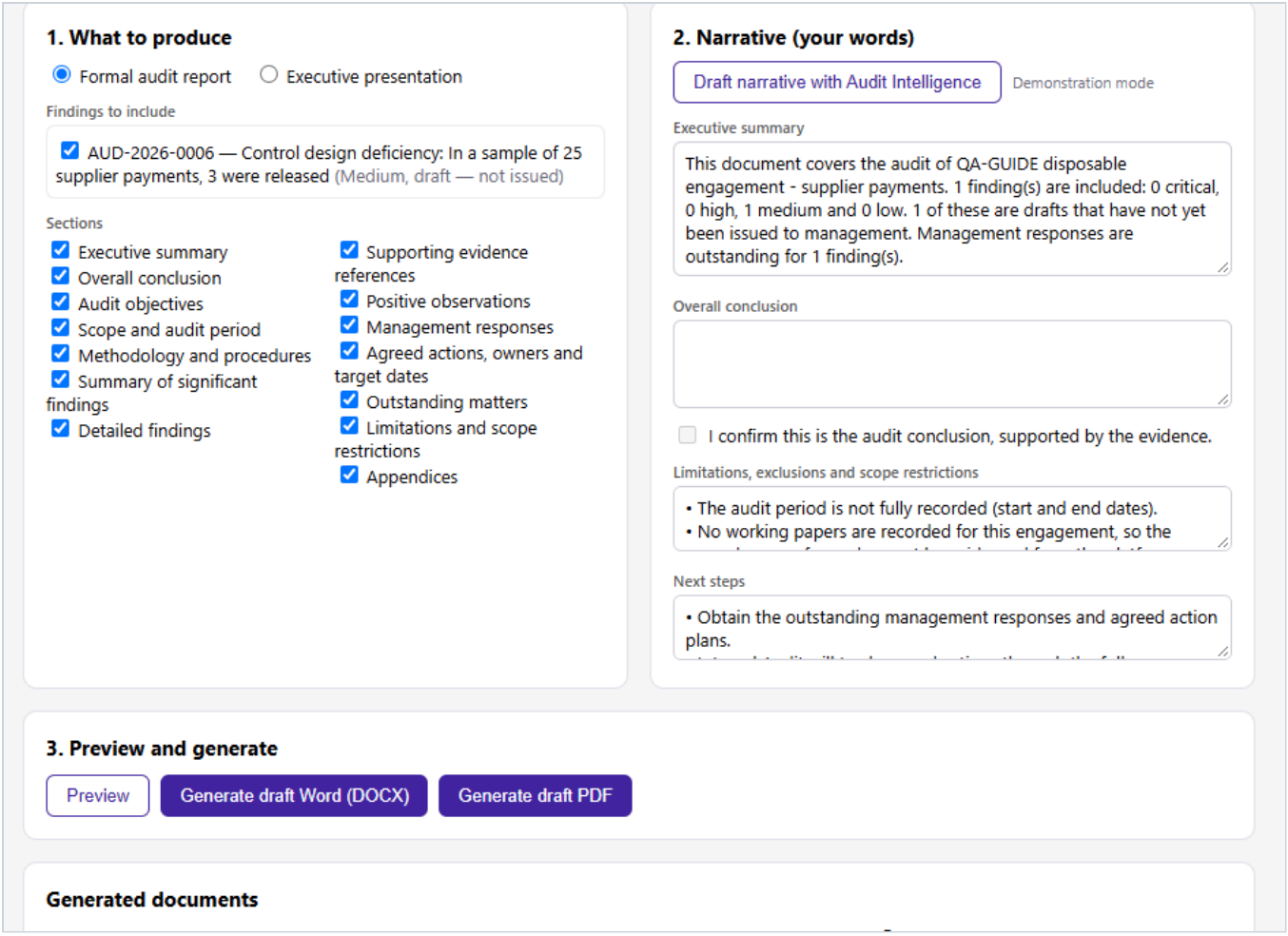


Figure 4 — Report narrative after “Use this draft”. The conclusion box is empty because the evidence did not support a proposed conclusion; the confirmation tick is unticked. Export buttons are in step 3.

E. Presentation narrative drafting

Purpose: the same narrative drafting for an executive presentation.

Path: the same page, choosing **Executive presentation** and an **Audience** (the audience changes emphasis only — never facts, ratings or conclusions).

Action: Draft narrative with Audit Intelligence. Review as in D; the extra field **Decisions or escalations required** (one per line) can be pre-filled by the draft.

Audit Intelligence drafts the **narrative text**. It does not design or generate the slides — see 11.5.

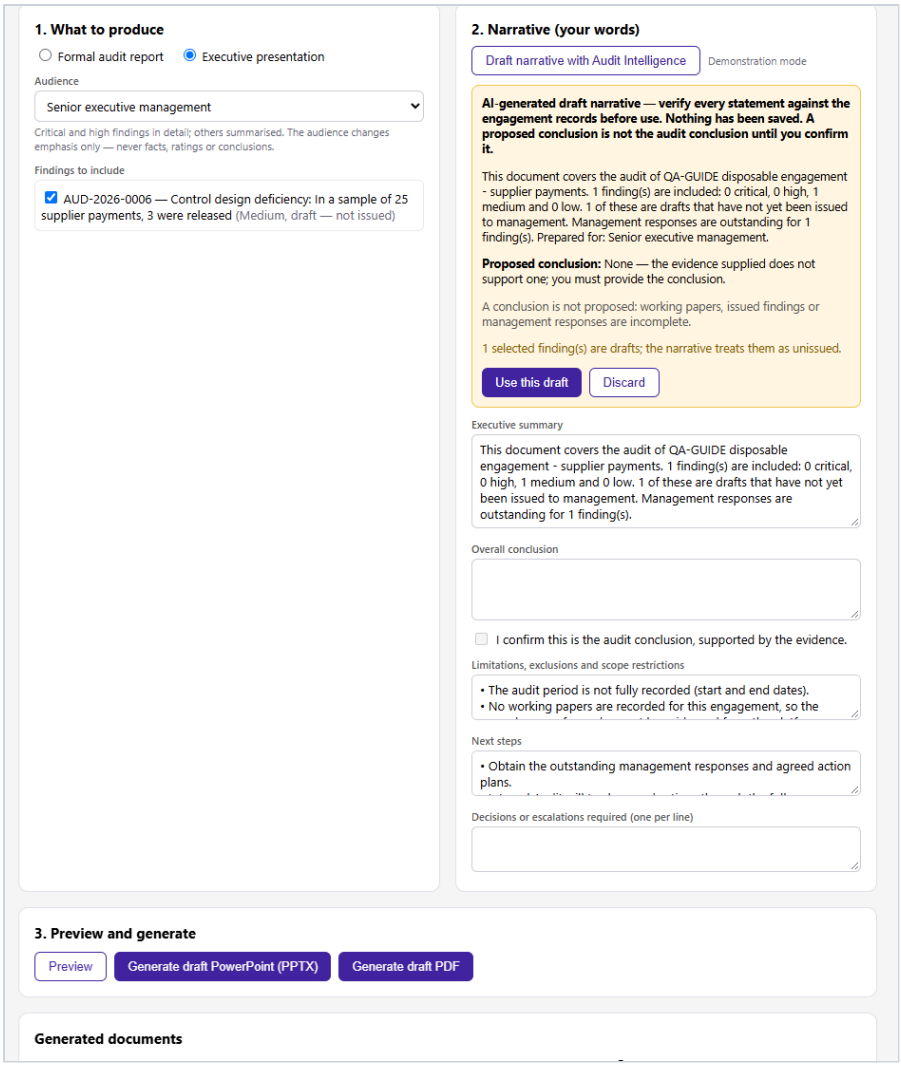


Figure 5 — Presentation narrative. The Audience selector changes emphasis only; export is by the separate PowerPoint (PPTX) and PDF buttons.

F. Audit program generation

Purpose: draft a risk-based audit program — a set of proposed procedures — for an existing engagement, as a structured starting point for your team.

Path: Engagements (`/engagements`) → open an engagement → ✦ **Generate Audit Program with Audit Intelligence**.

Input: none to type. The draft is built from the engagement's own details and from the active risks linked to the engagement's Audit Universe item (see "What is sent" below).

Availability: the button is offered on engagements that are not Closed, to users holding the permissions listed in 11.2. If the engagement **already has a linked audit program**, you can still generate a draft, but it is for reference only: it cannot be saved and never replaces or changes the existing program.

Step by step

1. Open the engagement and click ✦ **Generate Audit Program with Audit Intelligence**. The button reads "Generating audit program…" while the request runs.
2. The panel ✦ **Audit Intelligence audit program draft** opens, headed "AI-generated draft — review before saving". It shows a disclaimer and a note on the risk context used. If the draft used recorded risks, they are listed under **Risks used (from the Risk Register)**; risks with no recorded controls are marked "(no existing controls recorded)".
3. Under **Program**, edit the **Title**, **Audit Type**, **Objective** and **Scope**.
4. **Key Audit Areas**, **Overall Approach** and **Assumptions** are shown for your review only. They are **not saved** with the program.
5. Under **Procedures**, review each step. You can edit any field, reorder steps with ↑ / ↓, or **Remove** a step. Each step contains the fields in the table below.
6. Click **Save as engagement program** to save the program and link it to the engagement (the message "Audit program saved and linked to this engagement." confirms it). The saved program contains your edited wording and your final order. The button is unavailable if no procedures remain. Click **Discard draft** to throw the draft away.

Procedure field	What it holds
Procedure	The work to be performed (editable text).
Risk Addressed	The risk the step responds to. Where a step relates to a recorded risk, this is taken from that risk's title in the Risk Register, not from AI wording. Steps not tied to a recorded risk show the placeholder "General procedure".
Control Tested	The control the step tests, with a badge (see below).
Expected Evidence	The evidence the auditor expects to obtain.
Guidance Notes	Notes for the person carrying out the step.
Testing Method	Not specified, Inquiry, Observation, Inspection or Re-performance.
Sampling Method	Free text.

Control badge	Meaning
Recorded in Risk Register — not yet tested	The control text matches a control already recorded against the linked risk. It has not been tested.
Suggested control to validate — not verified	The control was suggested by Audit Intelligence. Confirm it exists before relying on it.

What is sent: the engagement's name, type, objective, scope, financial year, priority, overall risk rating and materiality; the Audit Universe item's name and description; and, for up to 15 active risks linked to that item, each risk's title, category, inherent and residual bands, causes, consequences and recorded existing controls. User

identities, team members, working papers, evidence, findings and audit logs are not part of the request. Engagements with no Audit Universe item receive no risk context, and the draft says so. Do not assume any of it stays local (see 11.4).

Limits: a draft is only as good as the engagement information supplied. Generation is refused on a Closed engagement and on a restricted engagement unless a System Administrator has allowed it (see 11.2). If the output cannot be validated you are asked to try again.

G. Audit program review
Purpose: have Audit Intelligence review an engagement's **existing** audit program — whether built manually, cloned from the library or generated — and suggest specific improvements for you to accept or ignore one by one.
Path: Engagements → open an engagement → ✦ **Review Audit Program with Audit Intelligence**.
Availability: the button appears only when the engagement has a **linked audit program** and is not Closed, to users holding the permissions listed in 11.2.
Key point: the review itself changes nothing. Suggestions start unselected, and accepted suggestions edit the existing program in place — they never replace it.

Step by step

1. Click ✦ **Review Audit Program with Audit Intelligence** ("Reviewing audit program…" shows while it runs).
2. The panel ✦ **Audit Intelligence program review** opens with an overall assessment badge — **Sufficient**, **Needs improvement** or **No program linked** — a summary, a disclaimer ("AI-assisted review — suggestions only. Nothing has been changed…") and a note on the risk context used. Up to the first 50 steps of a program are reviewed.
3. Read the findings sections (table below).
4. Tick the suggestions you want. Every one starts unticked. Each shows **CURRENT** next to **SUGGESTED** text, with a rationale.
5. Click **Apply selected (n)**. The platform re-reads the saved program first. Any suggestion whose original text has changed since the review is marked "Changed since the review — not applied" and is left out.
6. The remaining changes appear under **Changes to save (n)** as editable text. Edit them if needed. Nothing is saved yet. **Back to selection** returns to the suggestions.
7. Click **Save changes**. The selected edits are written to the existing program and the message "Selected changes saved to the audit program." appears. If something changed again while you were editing, that item is flagged and skipped. Click **Close review** to dismiss the panel without saving.

Part of the review	What it tells you
Program findings	Program-level observations, each with a severity.
Coverage of recorded risks	For each linked risk in the Risk Register, which step addresses it — or "not addressed by any step". Shown only when risk context was available.
Risks to consider	Suggestions only. They are **not** Risk Register entries and are not added to it.
Program header	Suggested changes to the program's own fields, shown as current versus suggested.
Steps	Each step has its own assessment badge (Sufficient or Needs improvement), findings and field-level suggestions. A Sufficient step with no suggestions shows "Adequate as saved — keep unchanged."
Suggested additional procedures	New procedures with testing method, expected evidence, control and a rationale. If you tick one and save, it is added as a new step.

What is sent: the engagement's details and the program's steps as saved. Where you hold Risk Register · View, the linked risks' context is included as well (as in F); without it the review runs without risk context. Suggested controls carry the same badges as in F and are not verified.

Limits: the review is refused on a Closed engagement and on a restricted engagement unless a System Administrator has allowed it. Output that cannot be validated returns the message "Audit Intelligence returned a review that could not be validated. Please try again." Audit Intelligence does not perform audit testing and does not execute the program. Your auditors must review, edit and validate every procedure before it is used.

11.4 Responsible use and information handling

- AI-generated content is a **draft**, not an approved audit conclusion.

- Verify facts, evidence, risk ratings, causes, recommendations and conclusions against your working papers before saving or issuing.
- Follow your organization's confidentiality and data-handling policies.
- **What leaves the platform depends on the workflow** and on the provider your environment is configured to use (your administrator can tell you which). Risk drafting sends the text you enter; finding generation sends your observation and the other inputs you provide, plus evidence file names; objectives and scope sends the engagement details and, where you can view the Risk Register, linked risk context; audit program generation sends the engagement details and linked risk context (see F), and audit program review sends the engagement details and the saved program steps, plus linked risk context where you can view the Risk Register (see G); report and presentation narrative sends structured engagement and finding data from the platform records. Do not assume any of it stays local. A screen showing a **Demonstration provider** badge or "Demonstration mode" is using built-in sample output that is illustrative only.
- Output can be incomplete or wrong. No accuracy level is guaranteed.
- Use clearly fictitious examples when learning; do not enter sensitive engagement data unless your policy allows it.

11.5 Reports and presentations: AI drafting vs. export

Audit Intelligence (AI drafting)	Platform export (not AI)
Drafts narrative text: summary, key messages, limitations, next steps, proposed conclusion, decisions required.	**Generate draft Word (DOCX)** / **PDF** for the audit report; **Generate draft PowerPoint (PPTX)** / **PDF** for the presentation. These assemble your findings and the narrative you approved into a file.
Does not generate slides or layout.	Generated documents are listed under **Generated documents** with a Draft status; **Finalise** creates a separate Final copy. Documents containing AI-drafted narrative are labelled "Audit Intelligence-assisted narrative".

A draft report narrative is not a finalized report or an approved conclusion. Export needs the Reporting · Export permission; without it you can preview only. A document is flagged "May be out of date" if the underlying records change after it was generated.

11.6 Troubleshooting and FAQ

Situation	What to do
I don't see any Audit Intelligence button	Check for the subscription notice, then your permissions (11.2). If neither explains it, Audit Intelligence may be switched off for the environment — contact your administrator.
"Not included in your subscription"	Your organization's package excludes it. An administrator can review the package under Admin → Organizations.
"Audit Intelligence is temporarily unavailable"	The provider did not respond in time or is unavailable. Your form is unchanged; try again later.
A limit message (minute / daily)	Wait a minute, or try again the next day.
Refused on a restricted engagement	The organization has not allowed restricted content to be processed externally (Admin → Restricted assignments).
Refused on a Closed engagement	Finding drafting, objectives and scope, audit program generation and audit program review are not available on Closed engagements. Reopen the engagement first.
I can generate an audit program but cannot save it	The engagement already has a linked audit program. Audit Intelligence never replaces it; the draft is for reference only. To improve the existing program, use **Review Audit Program** instead.

Situation	What to do
There is no Review Audit Program button	The engagement has no linked audit program, is Closed, or you lack Audit Programs · Edit (see 11.2).
A suggestion is marked "Changed since the review — not applied"	The program text changed after the review ran. Run the review again to get suggestions against the current text.
"…could not be validated. Please try again."	The generated program or review failed the platform's checks. Nothing was changed; try again.
Is the draft final?	No. Nothing is saved until you click Save Risk, Save as draft finding, Create Engagement / Save Changes on the engagement form, Save as engagement program, Save changes (program review), or generate a document.
"Save as draft finding" is disabled	Tick the verification checkbox first.

> SCREENSHOTS AND SOURCES
>
> Figures 1–5 were captured from a running test instance using the built-in demonstration provider, so the sample text is illustrative and not real model output. No screenshot of the subscription-restriction notice is included (it was not captured). Workflows F and G (audit program generation and review) have no screenshots; they are described from the application's screens and behavior, and the sample output shown by a demonstration provider is illustrative only. This guide documents only the Audit Intelligence actions listed in 11.2; it does not describe any other.